Strategy Research Project

AFCYBER: Postured to Support Air Force and USCYBERCOM Cyber Needs?

by

Colonel Jennifer P. Sovada
United States Air Force

United States Army War College
Class of 2013

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* xx-03-2013	**2. REPORT TYPE** STRATEGY RESEARCH PROJECT	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE AFCYBER: Postured to Support Air Force and USCYBERCOM Cyber Needs?	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Colonel Jennifer P. Sovada United States Air Force	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Mr. Brian A. Gouker Department of Military Strategy, Planning, Operations	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army War College 122 Forbes Avenue Carlisle, PA 17013	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 9,552

14. ABSTRACT

Based on the DoD goals for cyberspace and the need to ensure the DoD can operate freely in cyberspace and efficiently organize its resources, the Air Force has developed an institutional force devoted to supporting cyberspace operations, Air Force Cyber Command (AFCYBER). However, the Air Force is uncertain whether or not its cyber force is postured effectively to support cyber operations. This paper outlines the mission, posture, and organization of AFCYBER, discusses U.S. Cyber Command's (USCYBERCOM) mission and component command requirements as well as the missions and organizations of the sister Service cyber components, then compare these cyber components and missions to determine whether AFCYBER is postured properly to support the Air Force and USCYBERCOM missions and finally recommend how the Air Force's cyber component can align better with Air Force and USCYBERCOM needs to maximize Air Force personnel to support cyber missions.

15. SUBJECT TERMS
Intelligence, ARCYBER, Navy Fleet Cyber Command, Tenth Fleet, MARFORCYBER, N2/N6, 24 AF, AFISRA

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	UU	46	**19b. TELEPHONE NUMBER** *(Include area code)*

USAWC STRATEGY RESEARCH PROJECT

AFCYBER:
Postured to Support Air Force and USCYBERCOM Cyber Needs?

by

Colonel Jennifer P. Sovada
United States Air Force

Mr. Brian A. Gouker
Department of Military Strategy, Planning, Operations
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	AFCYBER: Postured to Support Air Force and USCYBERCOM Cyber Needs?
Report Date:	March 2013
Page Count:	46
Word Count:	9,552
Key Terms:	Intelligence, ARCYBER, Navy Fleet Cyber Command, Tenth Fleet, MARFORCYBER, N2/N6, 24 AF, AFISRA
Classification:	Unclassified

Based on the DoD goals for cyberspace and the need to ensure the DoD can operate freely in cyberspace and efficiently organize its resources, the Air Force has developed an institutional force devoted to supporting cyberspace operations, Air Force Cyber Command (AFCYBER). However, the Air Force is uncertain whether or not its cyber force is postured effectively to support cyber operations. This paper outlines the mission, posture, and organization of AFCYBER, discusses U.S. Cyber Command's (USCYBERCOM) mission and component command requirements as well as the missions and organizations of the sister Service cyber components, then compare these cyber components and missions to determine whether AFCYBER is postured properly to support the Air Force and USCYBERCOM missions and finally recommend how the Air Force's cyber component can align better with Air Force and USCYBERCOM needs to maximize Air Force personnel to support cyber missions.

AFCYBER:
Postured to Support Air Force and USCYBERCOM Cyber Needs?

> It is the intent of the United States Air Force to provide a full spectrum of cyberspace capabilities to Joint Force Commanders whenever and wherever needed. To this end, we have positioned the Air Force to confront the cyber-related challenges of today and tomorrow.
>
> —Michael B. Donley
> SECAF and General Norton A. Schwartz, CSAF
> August 20, 2009[1]

President Obama has identified cyber as one of the most important challenges the United States (U.S.) faces today because the adversary is seeking to exploit cyberspace to either cause downfall, detract, or degrade the U.S.' dominance throughout the world.[2] Currently the U.S. is unprepared to deal with the complexity of cyberspace, in particular how to protect it as well as use it to the nation's advantage.

Cyberspace is persistently contested and it is a domain through which the U.S. operates continuously; therefore, the U.S., in particular the Department of Defense (DoD), must understand how to protect, defend, deter, and assess the cyber domain.[3] Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, defines Cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[4] It further defines cyberspace operations as "The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[5] These two definitions show the complexity and diversity of cyberspace.

Due to this complexity and the importance of protecting our cyberspace equities, the Department of Defense (DoD) has allocated numerous resources to explore what the DoD and to some respect, the U.S. Government needs to do in the cyber realm. "The DoD operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe."[6] The DoD also uses cyberspace in its day-to-day operations to enable communications, intelligence, business processes, and other warfighting capabilities.[7] According to the DoD Strategy for Operating in Cyberspace, the goals of the DoD in cyberspace are to "take advantage of cyberspace's potential, … protect DoD networks and systems, … enable a whole-of-government cybersecurity strategy, … strengthen collective cybersecurity, [and] … leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation."[8]

Based on these DoD goals for cyberspace and the need to ensure the DoD can operate freely in cyberspace and efficiently organize its resources, the Air Force has developed an institutional force devoted to supporting cyberspace operations, Air Force Cyber Command (AFCYBER). However, the Air Force is uncertain whether or not its cyber force is postured effectively to support cyber operations. Lieutenant General Basla, the Air Force's Chief Information Officer, stated the Air Force needs to study whether or not its forces are organized properly.[9] This paper will outline the mission, posture, and organization of AFCYBER. Then it will discuss U.S. Cyber Command's (USCYBERCOM) mission and component command requirements as well as the missions and organizations of the U.S. Army, U.S. Navy, and U.S. Marine cyber components. This paper will then compare the Services' cyber components and missions to determine whether or not AFCYBER is postured properly to support the Air Force and USCYBERCOM missions and finally recommend ways the Air Force's cyber component can better align with Air Force and USCYBERCOM cyber needs to maximize the Air Force's and USCYBERCOM's use of Air Force personnel.

Air Force Cyber Command

The Air Force has a history of being founded on the interests of protecting and securing non-governed global commons such as cyberspace. In 1995 the Secretary of the Air Force Wynne and the Chief of Staff of the Air Force, General Moseley, jointly signed the Foundations of Information Warfare that defined the basis principles for Air Force operations in cyberspace.[10] Almost a decade later the Air Force added cyberspace into its mission statement because "adversaries will contest [the U.S.] across all of the domains: Land, Sea, Air, Space and Cyberspace. As Airmen, it is [the Air Force's] calling to dominate Air, Space, and Cyberspace."[11] This emphasis on cyber is demonstrated today when the Air Force identifies it as one of its core domains as stated in the Air Force mission: the mission of the United States Air Force is to fly, fight and win...in air, space and cyberspace.

The importance of cyber and the understanding that the Air Force needs to be able to defend and employ global cyber power, led the Secretary of the Air Force Wynne and the Chief of Staff of the Air Force, General Moseley, in September 2006 to order the establishment of an operational command for cyberspace.[12] These Air Force leaders wanted the Air Force to develop a plan to implement a new command that would organize, train and equip cyber forces; and conduct offensive and defensive cyber operations.[13] The Air Force Cyber Command current Strategic Vision further delineates what the Air Force wants its cyber mission to do. It describes the Air Force's vision as employing world-class cyberspace capabilities; controlling cyberspace; creating integrated global effects and delivering sovereign options.[14] Employing world-class cyberspace capabilities allows the Air Force to be an integral part of securing the nation from cyber threats. Controlling cyberspace helps the Air Force and the nation maintain and enhance its current advantages in "precision engagement, situational awareness, and operational reach."[15] Creating integrated cyberspace capabilities enables the Air Force to engage quickly and "degrade or destroy an adversary's terrestrial, air, and space infrastructure."[16] Finally, Air Force cyber is able to help the Air Force deliver sovereign options through employment of computer network exploitation, defensive cyber operations, and offensive cyber operations.

The organization that the Air Force created to execute this mission was 24th Air Force, a numbered Air Force under Air Force Space Command (AFSPC) and headquartered in San Antonio, Texas. The command declared full operating capability in October 2010 and in December 2010, the Air Force redesignated 24th Air Force as Air Forces Cyber (AFCYBER) to identify it as a Service component to USCYBERCOM.[17] The mission of 24th Air Force/AFCYBER is to "provide combatant commanders with trained and ready cyber forces to plan and conduct cyberspace operations, and to extend maintain and defend the Air Force portion of the global information grid."[18] This organization's roles, as described in Program Action Directive 07-08, Change 1, "Implementation of the Secretary of the Air Force Direction to Establish Air Force Cyberspace Command (AFCYBER)," are to serve as the lead for cyber-related *global vigilance* (network defense, network warfare support, network exploitation, and information assurance), *global power* (network attack, electronic warfare and cyber directed energy, information operations, network operations, and global command and control integration), *global reach* (in-garrison and expeditionary communication networks, data links, electromagnetic spectrum operations, and data integration) and *agile combat support functions* (command communication and information functions, engineering and installation, and electronic maintenance and evaluations).[19]

An Air Force Major General leads the command of approximately 5,400 active duty military, civilians and contractors as well as approximately 11,000 Air Reserve Component personnel.[20] The Air Force career specialties within 24th Air Force/AFCYBER consist of the enlisted career fields of cyberspace systems, cyberspace operations, and cyberspace defensive operations and for officers the cyberspace officer.[21] The Air Force does not consider electronic warfare, information operations or intelligence part of its cyber organization; however, it directs them to integrate with cyber.[22]

The command is comprised of four major sub-organizations; 624th Operations Center (624 OC), the 688th Information Operations Wing (688 IOW), 67th Network Warfare Wing (67 NWW), all located at Lackland Air Force Base, Texas and 689th Combat Communications Wing (689 CCW) at Robins Air Force Base, Georgia.

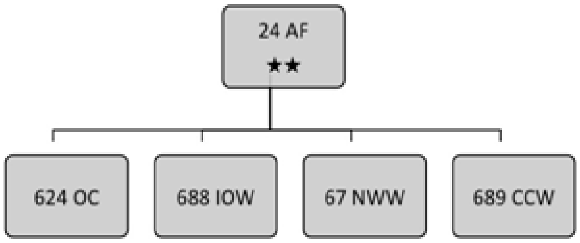

Figure 1: 24th Air Force Organizational Structure

The 624 OC is responsible for planning, directing, coordinating, assessing, and commanding and controlling cyber operations and capabilities in support of Air Force and Joint requirements.[23] The mission of the 688 IOW is to “deliver proven information operations and engineering infrastructure capabilities integrated across air, space and cyberspace domains.”[24] The 67 NWW “organizes, trains, and equips cyberspace forces to conduct network defense, attack, and exploitation.”[25] It also executes full spectrum Air Force network operations, training, tactics, and management for the Air Force Network Operations commander and combatant commanders. Finally, the 689 CCW trains, deploys and delivers expeditionary and specialized communications, air traffic control and landing systems for Humanitarian Relief Operations and dominant combat operations.[26]

The Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA) provides intelligence support to 24th Air Force/AFCYBER. AFISRA has a supporting relationship to 24th Air Force/AFCYBER where the 659th Intelligence, Surveillance, and Reconnaissance Group (659 ISRG) provides intelligence information to enable the cyber missions. This group, a subordinate unit to the 70th Intelligence, Surveillance, and Reconnaissance Wing (70 ISRW), is outside of the AFSPC and 24th Air Force/AFCYBER chain of command.

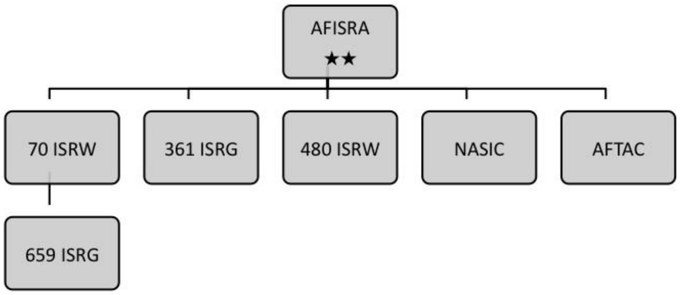

Figure 2: Air Force Intelligence, Surveillance, and Reconnaissance Agency Organization Chart

According to the 624th Operations Center Commander, Col Berry, 24th Air Force/AFCYBER and the 659 ISRG have a good working relationship; however the relationship is often strained due to the dual chains of command for the 659 ISRG because they conduct operations for both 24th Air Force/AFCYBER and the National Security Agency (NSA) as part of the 70 ISRW.

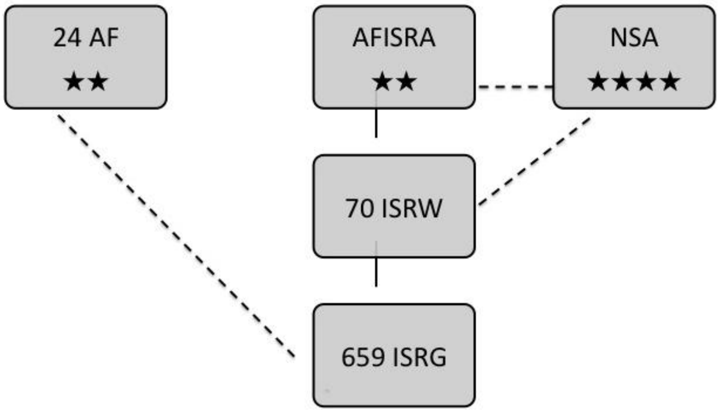

Figure 3: Command Relationship between 24th Air Force and 659th Intelligence, Surveillance, and Reconnaissance Group

Ultimately, 24th Air Force/AFCYBER supports Air Force and Joint Force commander cyber missions while integrating with other entities such as intelligence, electronic warfare, and information operations from other organizations.

The Air Force has developed a robust cyber training program to support its cyber mission. The Air Force uses an incremental approach that allows it to build on an Airman's previous experience and also them career path to determine which training the Air Force will provide them. The Air Force offers four primary courses for enlisted Airmen; undergraduate cyber training, network warfare bridge course, intermediate network warfare training, and mission qualification training.[27] For officers, the Air Force recently developed cyber training around 200-, 300- and 400-level course concept. The 200 level courses will update existing skills and introduce new skills, the 300 level courses will focus on joint cyber operations and strategic implications of cyberspace and the 400 level courses will discuss policy issues and refresh skills.[28] The Air Force has opened its 200 and 300 level courses to other services to avoid service-specific training and promote joint operations.[29] In addition to traditional courses, the Air Force has partnered with industry and the National Security Agency to allow government and civilian experts to teach Airmen their craft.[30] Also, it has developed "cyber ranges" where Airmen can practice their cyber skills in a closed environment without affecting live networks.[31] The Air Force has a vast array of training opportunities for cyber, and the training listed above is a small sample of what the Air Force offers. The Service continues to develop and advance its training as the domain continues to change.

Overall, Air Force cyber is in flux. General Welsh, the Chief of Staff of the Air Force, stated in September 2012 at the Air Force Association Convention that he "still twitches" when he says "cyber."[32] He believes cyber is a black hole with undefined requirements. He stated that the Air Force is going to slow down its advancement of cyber until he knows where the Air Force wants to go.[33] As a result, the Air Force held a cyber summit in November 2012 for over thirty Air Force senior leaders to include the Secretary of the Air Force, Chief of Staff of the Air Force, all four star Air Force Generals and many of the Headquarters Air Force Deputy Chiefs of Staff. The cyber summit addressed cyber issues, requirements, capabilities and gaps and attempted to establish a way forward for Air Force Cyber.[34] "The summit ensured senior Air Force leaders had the same understanding of cyber operations, the Air Force's cyber role, and Air Force cyber capabilities."[35] At the conclusion of the summit, Air Force leadership did not decide on a specific way ahead for cyber, but the information they gained has allowed them to begin addressing the major areas of concern to include mission, personnel, training, and capabilities in the cyber domain.

A key outcome from the cyber summit is that the Air Force needs to better understand the requirements from USCYBERCOM and what the other Services are doing to support USCYBERCOM and their own unique cyber missions so the Air Force can support all cyber missions.

U.S. Cyber Command

In June 2009, the Secretary of Defense Gates directed the commander of U.S. Strategic Command (USSTRATCOM) to establish a new sub-unified command under USSTRATCOM.

> [The U.S.'] increasing dependency on cyberspace, alongside a growing array of cyber threats and vulnerabilities, adds a new element of risk to our national security. To address this risk effectively and to secure freedom of action in cyberspace, the Department of Defense requires a command that processes the required technical capability and remains focused on the integration of cyberspace operations. Further this command must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners.[36]

This command is to be the lead cyber integrator and operator for cyber capabilities within the DoD. From this memorandum, USSTRATCOM established USCYBERCOM, the first U.S. warfighting command dedicated to how we organize, train, equip and operate in and through cyberspace. USCYBERCOM reached full operational capability in October 2010.[37]

The mission of USCYBERCOM is to plan, coordinate, integrate, synchronize and conduct activities to: "direct the operations and defense of specified [DoD] information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./Allied freedom of action in cyberspace and deny the same to our adversaries."[38] USCYBERCOM's headquarters is at Fort Meade, Maryland where it is co-located with the National Security Agency (NSA) to take advantage of the resident expertise, authorities and systems already in place to effectively and efficiently achieve the DoD's goals.[39] By 2011, USCYBERCOM had approximately 1,000 employees at the headquarters with a $150 million budget for fiscal year 2011.[40] The number of personnel in the command is expected to increase by 4,000 personnel, mostly military within the Service components. USCYBERCOM's budget is expected to grow as the Services and DoD recapitalize resources from other programs to fund cyber.[41]

The President of the United States has given USCYBERCOM three primary mission areas to consider at the strategic level to protect and defend the U.S. from cyber operations: supporting the geographic combatant commanders; protecting the global information grid (GIG); and defending the nation, in particular key components of industry.[42] To support these missions, USCYBERCOM has developed a structure called "national mission cyber teams" that will be able to provide a standardized force presentation to each mission area. Each team will have specific cyber core competencies that best support the mission areas. Supporting Geographic Combatant Commanders will require the cyber professionals to integrate cyber into operational planning and provide direct support to operations. Protecting the GIG will include distinct protection teams that will attempt to preclude an attack on the GIG. Finally, defending the nation will involve cyber national mission teams that would be multi-role, multi-function teams that would help protect the U.S.' critical infrastructure, banking system and other key components of U.S. industries.

In addition to these national mission teams, USCYBERCOM has outlined Service-retained niche capabilities, where each service will have unique mission sets to focus its Service-unique capabilities such as functional teams (e.g. integrated air defense systems, naval operations); tactical cyber teams (e.g. units deployed forward to combat area); and Service-provided computer network defense (e.g. Air Force Network Operations). Each of the national mission teams, with their Service-unique capabilities, needs to understand and be able to operate within USCYBERCOM's three lines of operation: GIG operations; defensive cyberspace operations; and offensive cyberspace operations to effectively support their team.[43]

To support USCYBERCOM's identified missions, the command has identified four areas where it and the Services need to improve their integration to enhance and advance these cyber missions. General Alexander, Commander USCYBERCOM, first envisions a cyber profession where communications, signals intelligence, cryptography, computer science, intelligence, and electronic warfare are one workforce.[44] He believes that combining the organization and operation of these disparate specialties will allow for better coordination, information cross flow and operational execution of cyber. Second, USCYBERCOM, in coordination with the Defense Information Systems Agency (DISA), should be responsible for developing a joint training standard for all cyber professionals, to include the Service cyber components, who operate within USCYBERCOM.[45] DISA has been determining "what [is] the appropriate training, skills and knowledge [to] work toward the development of more modularized training."[46] However, each Service has different training standards for its cyber professionals, and the DoD has not yet granted USCYBERCOM the authority to establish joint training standards; therefore, each service member has different capabilities based on where they attended training.[47] Third, USCYBERCOM has identified the need for legal authorities to conduct cyber operations that the USCYBERCOM commander holds that are distinct from the authorities NSA.[48] The DoD and Congress have oversight of all authorities within U.S. Codes Title 50 and Title 10. USCYBERCOM must have distinct authorities that clearly delineate what is authorized in cyber rather than relying on signals intelligence authorities. Finally, USCYBERCOM has identified a need for the command and the Services to reach an agreement on how the Services and USCYBERCOM will manage the forces working with USCYBERCOM. The Services and USCYBERCOM need to determine the command relationships for each component to ensure adequate support to USCYBERCOM, the combatant commanders, and each Service's unique mission set.

USCYBERCOM relies heavily on its Service components to provide the majority of the force structure it needs to conduct its missions; however, it is still maturing its interactions with the Services to best support the Geographic Combatant Commanders, protect the GIG and defend the nation. The Service components that are assigned to USCYBERCOM include AFCYBER, as previously discussed; Navy Fleet Cyber Command/Tenth Fleet; Army Forces Cyber Command (ARCYBER); and Marine Forces Cyber Command (MARFORCYBER).

U.S. Navy Fleet Cyber Command/Tenth Fleet

The Navy went through a significant organizational change to adapt to the changing intelligence and cyber environments. In October 2009, the Navy reorganized the Office of Naval Intelligence (N2) and the Communications Network Directorate (N6) into the Information Dominance Corps (N2/N6). The Navy designed this organization to integrate and innovate across the maritime, cyber, and information domains to address more completely the challenges of the information age.[49] Vice Admiral (VADM) Dorsett was the first Deputy Chief of Naval Operations for N2/N6. He was responsible for "making investment decisions for information, cyber and space capabilities, and for also developing the Navy's information architectures."[50] VADM Dorsett created an information dominance corps that was comprised of information specialists who came from individual communities such as intelligence, communications, electronic warfare, information warfare, space, meteorology, oceanography, and cryptology.[51] The unique characteristic of this corps is that all individual communities would unite, be managed and developed as one, and fight together.[52]

Simultaneously, the Chief of Naval Operations, Admiral Roughead, directed the Navy to establish Fleet Cyber Command and recommission Tenth Fleet as a sub-organization of the Information Dominance Corps. In January 2010, the Navy officially launched its cyber corps at Fort Meade, Maryland to "conduct full spectrum operations in and through cyberspace to ensure Navy and Joint/Coalition Freedom of Action while denying [the] same to [the U.S.'] adversaries."[53] This new organization also allows the Navy to "remain a leader in cyberspace operations and provide the command and control structure necessary to achieve decision superiority in the information domain."[54] Specifically, Tenth Fleet assumed administrative control and U.S. Fleet Cyber Command assumed operational control over the cyber warfare, network operations, information operations, cryptology, and space forces to properly align under USCYBERCOM.[55] In addition to its cyber-related missions, Tenth Fleet also serves as the Navy's Service Cryptologic Component (SCC) Commander to NSA. This allows Tenth Fleet to delegate closely held signals intelligence authorities to operational forces in its chain of command. The goal of having both cyber and SCC responsibilities is to allow Navy cyber forces the ability to provide "relevant, resilient, and effective Command, Control, Communications, Computers, Collaboration, and Intelligence capabilities … to maximize Fleet readiness and support all missions through cyberspace."[56]

The mission of Fleet Cyber Command is to "serve as the central operational authority for networks, cryptologic/signals intelligence, information operations, cyber, electronic warfare, and space capabilities in support of forces afloat and ashore."[57] This mission statement is unique because only the Navy has their cyber command direct both cryptologic/signal intelligence and cyber forces, thus allowing increased synergy across the closely aligned competencies. In addition, serving as the operational authority for the above mentioned capabilities, Fleet Cyber Command directs cyberspace operations; organizes and directs cryptologic operations; executes cyber missions; directs, operates, maintains, secures, and defends the Navy's portion of the Global Information Grid; delivers integrated cyber, information operations, cryptologic and space capabilities; prioritizes all requirements within Tenth Fleet's purview; assesses Navy cyber readiness; and organizes, trains, and equips all forces under its command.[58]

Fleet Cyber Command/Tenth Fleet has delineated three lines of operation for their forces. First, its forces will operate within the cyber domain to be able to navigate and work within cyberspace. Second, they will actively defend the Navy's ability to command and control operational forces in any environment. Finally, they will exploit and attack on "command and in coordination with Joint and Navy commanders [and] conduct operations to achieve effects in and through cyberspace."[59] These three lines of operation are aligned with USCYBERCOM direction for the Services.

A key aspect of the Navy's effectiveness within these lines of operation is its ability to move smoothly between the authorities within Title 50, War and National Defense and Title 10, Armed Forces of the U.S. Code. Title 50 authorities allow authorized users in the U.S. Government to analyze network activity of targeted users and or computers, analyze network activity of targeted groups, provide alerts when targets users/computers are active, track network usage, and determine associations of groups and individuals.[60] The NSA maintains this authority and delegates it solely to intelligence or cryptology individuals or organizations that have special training in how to legally handle this information. NSA also delegates Title 50 authority to the SCC, in this case the Fleet Cyber Command/Tenth Fleet commander. Title 10 allows authorized users of the U.S. Government to deny network and/or computer use, degrade network and/or computer use, redirect network traffic, and disrupt or destroy data/computers while it also limits the U.S. Government's ability to collect and store intelligence data on U.S. persons.[61] The general-purpose warfighting forces operating within the DoD use Title 10 authorities daily to conduct their missions. For the Navy, the Fleet Cyber Command/Tenth Fleet commander is also responsible for Title 10 authorities and conduct. Since the commander of Fleet Cyber Command/Tenth Fleet has responsibility for both U.S. Code Title 50 and Title 10, he is able to integrate his forces and work more effectively within the cyberspace domain. He has the ability to task and manage his forces to ensure personnel with the ability to execute all aspects of these Titles are available to conduct the mission without delay.

Title 50 and Title 10 authorities under one commander give the Navy unprecedented flexibility and effectiveness to conduct the cyberspace mission. The Navy has allocated a large subset of the Information Dominance Corps,' approximately 46,000 personnel assigned to various units within Tenth Fleet and Fleet Cyber Command, to execute the mission in accordance with the lines of operation and within the legal limits of U.S. Code.[62]

Fleet Cyber Command/Tenth Fleet has six standing task organizations—Headquarters Element; Service Cryptologic Component Operations; Information Operations; Research and Development; Network Operations and Defense Group; and Fleet and Theater Operations. Each of these organizations is aligned to one of more of the lines of operation with integrated members of the Information Dominance Corps as the operators. For example, the Service Cryptologic Components have personnel within their organizations that specialize in cyberspace operations, electronic warfare and cryptology that are able to operate, defense and exploit/attack in the cyberspace domain. These professionals work together to accomplish the mission and to ensure compliance with U.S. Code and delegated authorities while maintaining safety and security for the U.S.

The U.S. Navy is ahead of the other Services in training cyber professionals. Vice Admiral Rogers, Commander U.S. Fleet Cyber Command, stated to the House Armed Services Committee, that the Navy has supported the DoD and USCYBERCOM efforts to create standards to develop a professional cyber force; however, DoD and USCYBERCOM have made little progress in establishing the training to support the standards. In the interim, the Navy has developed a tiered training strategy to train cyber professionals based on what the individuals will be doing and where they will be working.[63]

> The first tier focuses on building cyber awareness across all users on cyber threats and the role of cyberspace in naval operations. The second tier is tailored towards leadership and focuses on their responsibilities for Navy networks and building accountability for the application of offensive and defensive cyber capabilities. The third tier is designed to build a professional cyber workforce, ensuring they develop and maintain the expertise necessary to conduct effective cyberspace operations across the full range of military operations.[64]

The Navy includes both formal and informal training, and schoolhouse and virtual training to enable cyber professionals and their leaders stay apprised of the "latest threats and technology advances while mitigating cost and the loss of key personnel from units for an extended period of time."[65]

U.S. Army Cyber Command

In October 2010, in response to the stand up of USCYBERCOM and the need for a separate Army cyber organization, the U.S. Army reactivated 2nd Army and designated it U.S. Army Cyber Command (ARCYBER) at Fort Belvoir, Virginia.[66] "Army Cyber Command capitalizes on existing Army Cyber Command resources and achieves efficiencies by bringing cyber resources under a single command."[67]

The Mission of Army Cyber Command/2nd Army is to plan, coordinate, integrate, synchronize, direct and conduct network operations and defense of army networks; when directed conducts cyberspace operations in support of full spectrum operations to ensure U.S./Allied freedom of action in cyberspace, and to deny the same to our adversaries.[68] ARCYBER's roles are to: organize, train and equip Army cyber forces; defend all Army networks; integrate cyberspace into planning and exercises; provide cyber education training, and leader development to Army cyber forces; build partner capacity; conduct information operations for the Army; and be a cyber proponent to develop the future Army cyber force and develop a concept for land cyber unified operations.[69]

A Lieutenant General commands ARCYBER and serves as the Army Service component commander to USCYBERCOM as well as the Service Cryptologic Component commander to the NSA. Four organizations are subordinate to ARCYBER: the Network Enterprise Technology Command (NETCOM), 1st Information Operations (IO) Command (Land), the 780th Military Intelligence (MI) Brigade and the U.S. Army Intelligence and Security Command (INSCOM).[70] NETCOM is the Army's information technology provider for all network communications for the Army and maintains and defends the Global Network Enterprise. 1st IO Command (L) is a full spectrum IO organization "engaged from information operations theory development and training to operational application across the range of military operations."[71] The 780th MI Brigade is the newest cyber organization within ARCYBER and it conducts signals intelligence, computer network operations and computer network defense operations for Army and DoD networks.[72] Finally, INSCOM is primarily an intelligence organization that conducts intelligence, security, and information operations. It is under the operational control of ARCYBER for cyber-related actions.

> The streamlined command enables Army Cyber Command forces to capture efficiencies, increase effectiveness, pursue innovation and aggressively develop/refine operating procedures that affect the Army's global operational posture. The fusion of network defensive posture, threat activity and response capabilities to take pre-approved decisive action at "net speed" enhances ensures U.S./Allied freedom of action in cyberspace and to deny the same to our adversaries.[73]

The total command strength exceeds 21,000 personnel including soldiers, civilians, and contractors is expected to grow as the USCYBERCOM requirements grow even with the drawdown in overall force structure for the Army.[74]

ARCYBER believes its cyberspace operations include building, operating, defending, exploiting and attacking in cyberspace.[75] ARCYBER is looking to enhance these capabilities. First ARCYBER will integrate and synchronize cyberspace operations with electronic warfare, electromagnetic spectrum operations, information operations, and space operations to achieve commander's objectives to ensure mission command.[76] Also, it wants to increase its ability to conduct cyber unified operations and support the U.S. Army's "shape, prevent, and win" pillars with cyberspace capabilities through improved indications and warning, operational preparation of the environment, critical infrastructure protection, theater security cooperation, and integrating cyberspace operations into planning and targeting processes.[77] All of these goals are to establish the U.S. Army as a leader in cyberspace especially with respect to training and leadership development.

The U.S. Army believes personnel, not technology, are the key to advancing its cyberspace capabilities and therefore it must concentrate on organizing and training its cyber force for success. ARCYBER continues to evaluate its force structure and organization. ARCYBER identified a deficiency in its ability to support USCYBERCOM at Fort Meade, Maryland because it did not have the force structure in place responsively to support USCYBERCOM's needs. Therefore, ARCYBER established the 780th MI Brigade to be co-located with USCYBERCOM at Fort Meade, Maryland to enable closer ties to USCYBERCOM initiatives, training, and expertise. Prior to establishing the 780th MI Brigade, traditional signals intelligence units were dual-hatted to support both the NSA and USCYBERCOM. Now, the new brigade allows ARCYBER to be more flexible and understand the rapidly developing mission and organization of USCYBERCOM.

Also, the U.S. Army continues to evaluate its cyber training. Lieutenant General Hernandez, the commander of ARCYBER, stated:

> [The] national and military dependence on the cyber domain and information technology demands that [ARCYBER] invest in cyber capabilities to grow the skills necessary to maintain our ability to operate freely in cyberspace. … [ARCYBER] must therefore make significant investments in education, training, and experience to understand emerging trends, develop and deploy new capabilities and effectively defend against new cyberspace threats.[78]

ARCYBER has established the Army proponent office for cyberspace that is working with the Army Training and Doctrine Command (TRADOC) on how to best train its cyber forces. The U.S. Army wants to ensure that it is training, organizing, and equipping to meet the requirements from both the Service and USCYBERCOM.

U.S. Marine Forces Cyber Command

The U.S. Marine Forces Cyber Command (MARFORCYBER), led by a Lieutenant General, has the smallest cyber component with fewer than 300 personnel.[79] However, the Marine Corps leverages the Navy for the majority of its training due to lack of resources and expertise which may account for the lower numbers of Marine cyber personnel. MARFORCYBER achieved initial operating capability in October 2009, declared full operating capability in January 2010 and is headquartered at Fort Meade, Maryland. It is focused on supporting the Marine Corps with providing about ten percent of its forces to the joint force commanders through USCYBERCOM for the greater cyberspace mission.[80] MARFORCYBER's mission is to:

> Plan, coordinate, integrate, synchronize and direct full spectrum Marine Corps cyberspace operations to include DoD Global Information Grid Operations, Defensive Cyber Operations, and when directed, plan and execute Offensive Cyberspace Operations, in support of Marine Air Ground Task Force, joint and combined cyberspace requirements in order to enable freedom of action across all warfighting domains and deny the same to adversarial forces.[81]

It is organized into three sub-organizations. First, it contains a command element that conducts administrative support to the cyber force. Second, it contains a Marine Corps Network Operations Security Center that focuses on supporting and protecting the Marine Corps network. Finally, it has a company from the Marine Corps Cryptologic Support Battalion to aid in cyberspace operations execution.

Different from the other services, Marine Corps cyber professionals will be riflemen first and foremost. Col Zotti, Chief of Staff for MARFORCYBER, stated that "while there will be some associated skills for cyber, they will remain Marines first, cyber warriors second."[82] He amplifies his comments by asserting, "cyber has to be heavily integrated with all warfighting functions because all are critically dependent on cyber for speed, precision, and lethality. So the [Marine's] success … is based on how well [it] can integrate it, not on creating a stand-alone capacity."[83] To achieve its goal for developing cyber warriors, the Marine Corps has developed rudimentary cyber training for its professionals. In particular, the Service has a cyber primer course that provides basic computer network operations and a Marine Corps Communication-Electronics School that does specialized training.[84]

Comparison

All of the Services have unique approaches to cyberspace. They have based their organizational, training, and resourcing decisions on how they want to contribute to the cyber mission. Each Service is wrestling with organization, force presentation, and training. With respect to training, each Service is trying to determine how much training should be Service-specific and how much should be joint. Additionally, the Air Force and the Army are struggling with how to organize to present forces to USCYBERCOM, while still maintaining their Service integrity and interests related to their Service-unique cyber missions. The Air Force and Army are also considering ways to facilitate and use the authorities resident within their Services to enable execution of cyberspace operations and protection. It seems that the Navy has started to conquer these two issues with its reorganization to the N2/N6 model, but it still has drawbacks and limitations it must work out. All of the Services continue to evolve their philosophies. The Air Force is taking a hard look at all aspects of its cyber mission; however, the Air Force needs to think of ways to revolutionize cyber rather than just evolve.

Recommendations

The Air Force has significant cyber experience. According to General Lord, former Air Force Cyberspace Command (Provisional) Commander, its "global perspective, technological acumen, effects-based approach, and emphasis on operations in the domain as primary options for achieving national goals … [shapes] how [the Air Force builds] toward access, influence, and control in cyberspace."[85] The Air Force does not seek to usurp any other Services' authority nor does it claim exclusivity in cyberspace; however, it desires a cyberspace force that can create effects and enable the Air Force to fight in air, space, and cyberspace.[86] Therefore, the Air Force must transform how it approaches cyberspace to effectively enable its cyber mission while supporting USCYBERCOM's mission. The Air Force must transform in six areas: how it thinks about cyberspace; cyberspace training; authorities; personnel management; force presentation; and overall organization of forces.

First, the Air Force must change how the Service as a whole views cyberspace. It needs to see cyber as a core competency and a warfighting domain beyond what is stated in the Air Force mission statement. All of the Air Force, from pilots to planners, need to understand cyber capabilities and potential effects as well as where cyber should fit into planning processes, defense of the Nation, and overall day-to-day Air Force operations. In addition, the Air Force must lead the other Services in cyber and cyber-related thinking because of our history of innovation and an entrepreneurial culture as well as our long history with cyber compared with the other Services. The Air Force should lead the other Services to better understand cyber-effects based operations so the joint force can effectively and efficiently conduct joint operations in the cyber realm. The Services must understand that cyberspace options support the effects you create and the impact you have in cyberspace and in the physical domain, not how quickly you achieve an effect.

Second, the Air Force must transform its cyber training to ensure it has properly trained Airmen to support both USCYBERCOM and Air Force requirements. General Alexander considers having trained and ready forces as the single most important focus for USCYBERCOM.[87] To support his vision, Airmen must be “full-spectrum professionals [that] employ core cyberspace capabilities across the entire range of military operations.”[88] To achieve this, the Air Force needs work with USCYBERCOM, vice independently, to develop joint training standards as well as evaluate its current Air Force cyber training. Working with USCYBERCOM to develop joint training standards that incorporate many of the Air Force training best practices and techniques that apply to the larger cyber force will benefit the Air Force and USCYBERCOM. They will also benefit the larger cyberspace enterprise to include the other Services, DoD entities and non-government organizations and businesses. These joint training standards will allow for sharing training materials, techniques, and certification processes that in the long run will reduce redundancy while still developing the best training. The Air Force should train its Airmen supporting USCYBERCOM missions to these standards once USCYBERCOM validates the training. According to General Alexander, Commander, USCYBERCOM, training to a common standard is one of his main priorities for all Services. “Combatant Commanders need to know that when they ask for a cyber capability, it does [not] matter whether the Army, Navy, Air Force or Marine Corps responds—they will get the capability they require.”[89] He also stated that USCYBERCOM must “establish training and certification standards for teams to be capable of operating, defending and attacking in cyberspace.”[90] Additionally, the Air Force needs to evaluate whether or not its current training is suited to the niche missions of the Air Force in cyberspace. Lieutenant General Basla, Air Force Chief Information Dominance and Chief Information Officer, stated that current Air Force training is not meeting the demand for the number of Airmen that must attend and complete training to meet Service and USCYBERCOM requirements.[91] Therefore, he has asked the Air Force to determine whether or not the training needs to increase or change to meet these new requirements. The Air Force must evaluate cyber training not only to ensure it is presenting fully trained and operational forces to operate in the cyberspace domain but also so that its training is developing joint cyber leaders who have specialized skills and cyber understanding to lead the joint cyberspace force in the future. The Air Force faces three challenges when evaluating its training. First, the Air Force's reevaluation of training may cause is a realization that the Air Force needs to revamp its training. Second, the cost to revamp training may be cost prohibitive to the Air Force especially in this budget-constrained environment. Finally, USCYBERCOM may require the Air Force to pay a portion of the overall cost to develop, update, or perform joint training. Once again, the cost may not be feasible for the Air Force to fund.

Third, the Air Force, with the other Services, must work diligently with the NSA and USCYBERCOM to facilitate their delegation of authorities to Service units and missions. General Alexander stated "while needed authorities may exist within the executive branch, [USCYBERCOM] currently lacks the delegated, implemented authority to perform all of the activities necessary to defend the nation in cyberspace."[92] Air Force cyber operations need the ability to fluidly move between U.S. Code Title 50 and Title 10 responsibilities for both NSA and USCYBERCOM delegated missions and Air Force specific missions. The Air Force needs to be able to operate with minimal oversight from NSA with combined cyber and intelligence forces to conduct defensive cyberspace operations to protect and defend its Service-owned networks. Currently, the Air Force does not fully understand the process and limitations for requesting and maintaining these authorities; therefore it is imperative the Air Force, in concert with the other Services, works with both NSA and USCYBERCOM to outline procedures for the Air Force to obtain the needed authorities. In the long run, all services and these agencies will benefit. A disadvantage of Air Force autonomous operations is that the Service may loose insight into new USCYBERCOM missions because it will be focused on Air Force requirements rather than the needs of the cyber community. In turn, the Air Force may lose its technological and analytical advantage in cyber because of the division in responsibilities.

Personnel management is the next area the Air Force needs to evaluate. The recent Cyber Summit identified the need to determine which career fields are "in" cyber and which are not. Secretary of the Air Force Donley, stated in October 2012, the Air Force should "broaden [its] view of cyber … and integrate across disparate realms such as cyber, signals intelligence and electronic warfare to achieve integrated effects."[93] Currently, the Air Force has designated a limited number of career fields as cyber with several career fields such as intelligence, space and others as supporting cyber. Because the Air Force does not include these other career fields in their definition of cyber, they are often excluded or forgotten when the Air Force attempts to conduct cyber operations. Consequently, the Air Force needs to evaluate the Navy's N2/N6 model and develop a cadre of information warfighters who are better integrated to support all cyber-related core competencies. For example, Brigadier General Franz, USCYBERCOM /J3, stated "cyber informs intelligence and intelligence informs cyber," so why should the Services not have better integration and organization to develop and take advantage of these relationships.[94] Lieutenant General Basla believes cyber is a team effort that requires numerous functional areas such as engineers, intelligence, acquisition, and cyber operators to work together.[95] At a minimum, the Air Force should consider integrating, but not combining, cyber and intelligence into a corps such as the Navy N2/N6 to start to institutionalize the appreciation that these functional areas are integrated and reliant on each other. Integrating cyber and intelligence may create the same issue that the Navy's N2/N6 currently has where the integration has been difficult and the two communities have not embraced their new structure and really begun to work together.

Another personnel concern the Air Force needs to evaluate is force presentation for USCYBERCOM missions. Force presentation is what command authorities the Air Force allows USCYBERCOM to control over its Airmen working directly for USCYBERCOM. The Air Force can retain operational control (OPCON) and/or administrative control (ADCON). Historically, the Air Force has retained ADCON and given OPCON to other organizations such as NSA for the majority of its forces. This command and control structure has allowed organizations, such as NSA, to utilize Airmen in whatever mission or manner it deems. In turn NSA has been able to train its personnel to a common standard, provide them enhanced technical expertise, and develop team cohesion based on common goals and operational objectives. However, this also has the potential to create a situation where Airmen work outside of their area of expertise and in areas such as analyzing naval submarine forces and ground maneuver units. The Air Force needs to reverse the ratio of Airmen that are OPCON to USCYBERCOM and develop a force structure akin to the U.S. Special Operations Command (USSOCOM) where the majority of USSOCOM forces are in direct support of combatant commanders. Joint Publication 1-02 defines direct support as “a mission requiring a force to support another specific force and authorizing it to answer directly to the supported force’s request for assistance.”[96] Organizing forces to be direct support allows for USCYBERCOM to direct missions the Airmen support, but also allows the Service to reallocate its personnel to missions that better utilize the Service-specific unique capabilities. It also allows the Air Force to emphasize missions that are mutually beneficial to both the USCYBERCOM and the Air Force. If the Air Force changes its force presentation to USCYBERCOM, it may lose influence within the command to help with advancing the missions, technology, and emphasis for cyber forces so the Air Force needs to ensure it is continuously dialoguing with USCYBERCOM on its way ahead.

Finally, the Air Force needs to reorganize to maximize the potential for mutli-domain, multi-function integration. Lieutenant General Basla questions whether or not the Air Force was organized properly to facilitate the teaming and integration.[97] 24th Air Force/AFCYBER and AFISRA need to combine into one major command (MAJCOM), the Air Force Information and Intelligence Command (AFIIC).

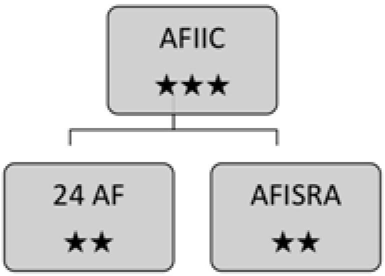

Figure 4: Proposed Air Force Information and Intelligence Command

AFIIC would remove 24th Air Force/AFCYBER from being a subordinate unit to AFSPC and remove AFISRA as a field operating agency subordinate to Headquarters Air Force, Directorate for Intelligence (HAF/A2). This command would be similar to the Navy's N2/N6 concept except that it would only include the Air Force's cyber and intelligence forces that currently reside within 24th Air Force/AFCYBER and AFISRA. The commander would be the AFCYBER component commander instead of 24th Air Force. 24th Air Force would be the execution arm of AFCYBER. A Lieutenant General should lead the command, as the AFCYBER Program Action Directive 07-08 originally directed, so that the commander can have equal rank to his/her sister-Service components.[98] This will allow equal representation to the USCYBERCOM commander from each Service. The headquarters should be at Fort Meade, Maryland to facilitate easier coordination with both USCYBERCOM and HAF/A2. AFISRA would become a separate Numbered Air Force (NAF) and would relinquish its SCC authorities to the MAJCOM commander. Allowing the MAJCOM commander to have U.S. Code Title 50 authorities would allow both cyber and intelligence forces delegated authorities directly from the MAJCOM commander. In turn this would facilitate successful mission execution, in particular for missions to defend its network and where the Air Force is the sole mission proponent. Combining these two organizations into one MAJCOM also allows for direct support between each NAF depending on what missions each was executing. AFIIC would also allow for smoother movement of personnel between the NAFs to increase exposure and experience of both intelligence and cyber operators. Personnel in each functional area would gain greater appreciation of what the other mission accomplishes and would stimulate ways to integrate better. Overall, AFIIC would reduce redundancy, improve efficiency and create an organization for overall better unity of command. There are several possible consequences of creating a new MAJCOM. First, the Air Force's creation of a new MAJCOM may cause the collapse of AFSPC because it would lose approximately fifty percent of its mission with the removal of its cyber responsibility. Also, the cyber and intelligence communities may not have a three or four star general that is familiar with cyber and intelligence to lead the force effectively. Combining the two may lead to a loss of leadership billets because the Air Force would be combining two organizations, while creating a requirement for more billets to create another staff structure. Finally, the intelligence and cyber career fields may conflict over which career field should command and lead this new MAJCOM.

Conclusion

The Air Force is at a crossroad with its cyber posture. It has unlimited potential to lead all Services into the future of cyber operations; however, it needs to decide how best to posture its cyberspace forces to support USCYBERCOM and Air Force missions. The Air Force can choose to stay its current course, or it can choose to revolutionize the way the Service thinks about and integrates cyber. If it wants to revolutionize, it will need to reevaluate and change how it conducts cyberspace operations, cyberspace training, authorities, personnel management, force presentation, and overall organization of forces. Once the Air Force moves forward and embraces this change, the Air Force will be postured to support both Air Force and USCYBERCOM cyber needs.

Endnotes

[1] U.S. Secretary of the Air Force Michael B. Donley and Gen Norton A. Schwartz, Chief of Staff of the U.S. Air Force, "Air Force Cyberspace Mission Alignment," memorandum for all Airmen, Washington DC, August 20, 2009.

[2] President Barack A. Obama, *Comprehensive National Cybersecurity Initiative* (Washington, DC: The White House, March 2010), 1.

[3] Michael Donley, Secretary of the Air Force and Mark Maybury, "Air Force Cyber Vision 2025, Assuring the advantage in air, space and cyberspace," October 2012, http://www.armedforcesjournal.com/2012/10/11492950 (accessed October 25, 2012).

[4] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010 (As Amended Through January 31, 2011)), 98.

[5] Ibid., 99.

[6] *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC, July 2011), 1.

[7] Ibid., 1.

[8] Ibid., 5, 6, 8, 9, 10.

[9] Jared Serbu, "Air Force Role Just 1 Piece of DoD's Cyber Puzzle," FederalNewsRadio.com, December 3, 2012. www.federalnewsradio.com/index.php?nid=851&sid=3140801 (accessed December 4, 2012).

[10] Jason Healey, "Claiming the Lost Cyber Heritage," *Strategic Studies Quarterly,* Fall 2012, 12.

[11] Secretary of the Air Force Michael W. Wynne and General Michael T. Moseley, Chief of Staff of the United States Air Force, "To the Airmen of the United States Air Force," Washington, DC, December 7, 2005.

[12] Secretary of the Air Force Michael W. Wynne and General Michael T. Moseley, Chief of Staff of the United States Air Force, "Establishment of an Operational Command for Cyberspace," memorandum for commanders of Air Combat Command, Air Education and Training Command, Air Force Material Command, and Air Force Space Command, Washington, DC, September 6, 2006.

[13] General Michael T. Moseley, Chief of Staff of the United States Air Force, “Operational Cyberspace Command “Go Do” Letter,” memorandum for 8th Air Force Commander, Washington, DC, November 1, 2006.

[14] Air Force Cyber Command, *Air Force Cyber Command Strategic Vision* (Barksdale AFB, LA: Air Force Cyber Command, February 2008), 3-4.

[15] Ibid., 7.

[16] Ibid., 8.

[17] 24th Air Force, “24th Air Force Fact Sheet,” May 2012.

[18] 24th Air Force, “Mission Statement,” August 15, 2012, https://www.my.af.mil/gcss-af/USAF/ep/contentView.do?contentType=EDITORIAL&contentId=c2D8EB9D633ACA2BF0133CC0AB09E05D3&channelPageId=sF575FC8E22DC74AF0122EB3ACE5D033B&programId=t2D8EB9D633ACA2BF0133CC066BC805D2 (accessed November 12, 2012).

[19] U.S. Department of the Air Force, *Implementation of the Secretary of the Air Force Direction to Establish Air Force Cyberspace Command (AFCYBER),”* Program Action Directive 07-08, Change 1 (Washington, DC: U.S. Department of the Air Force, January 24, 2008), 4-5.

[20] 24th Air Force, “24th Air Force Fact Sheet,” May 2012.

[21] HQ AFPC/DPSIDC, *Air Force Enlisted Classification Directory (AFECD), The Official Guide to the Air Force Enlisted Classification Codes* (Randolph AFB, TX: Air Force Personnel Center, August 1, 2012), 40, 195.

[22] David A. Fulghum, “Cyber-Scrimmage,” *Aviation Week and Space Technology*, vol 172, no. 19 (May 17, 2010): 26.

[23] 624th Operations Center Home Page, https://www.my.af.mil/gcss-af/USAF/ep/globalTab.do?channelPageId=sA1FBF31D23C34A850123C9CE6173015B (accessed December 12, 2012).

[24] 688th Information Operations Wing Home Page, https://www.my.af.mil/gcss-af/USAF/ep/globalTab.do?channelPageId=sF575FC8E22DC74AF0122EB46C3C703C8 (accessed December 12, 2012).

[25] 67th Network Warfare Wing Home Page, https://www.my.af.mil/gcss-af/USAF/ep/globalTab.do?channelPageId=s6925EC1352B80FB5E044080020E329A9 (accessed December 12, 2012).

[26] 689th Combat Communications Wing Home Page, http://www.24af.af.mil/units/689ccw/index.asp (accessed December 12, 2012).

[27] Amber Corrin, “Cyber Programs at a Glance,” FCW (November 17, 2011). http://fcw.com/articles/2011/11/28/feat-military-cyber-training-side-overview.aspx (accessed December 4, 2012).

[28] Henry Kenyon, "Air Force Emphasizes Skills Training for Cyber Personnel," Defense Systems (January 27, 2012). http://defensesystems.com/Articles/2012/01/27/Air-Force-Emphasizes-Skills-Training-For-Cyber-Personnel.aspx?Page=1 (accessed December 12, 2012).

[29] Ibid.

[30] Amber Corrin, "Cyber Training No Longer Basic," FCW (November 17, 2011). http://fcw.com/articles/2011/11/28/feat-military-cyber-training.aspx (accessed December 4, 2012).

[31] Ibid.

[32] General Mark Welsh, Chief of Staff of the United States Air Force, "Speech to Air Force Association Convention," September 18, 2012. *YouTube*, video file. http://www.youtube.com/watch?v=FyCoISvM_4U (accessed September 27, 2012).

[33] Ibid.

[34] Air Force Public Affairs Agency, "Q&A: AF Chief Information Officer on Cyber Summit," December 11, 2012, Air Force News, http://www.af.mil/news/story.asp?id=123329468 (accessed December 12, 2012).

[35] Ibid.

[36] Secretary of Defense Robert M. Gates, Memorandum for Secretaries of Military Departments, Washington, DC: Office of the Secretary of Defense, June 2009, 1.

[37] General Keith B. Alexander, *Building a New Command in Cyberspace* (Maxwell AFB, AL: Air University, Strategic Studies Quarterly, Summer 2011), 3.

[38] U.S. Department of Defense, *U.S. Cyber Command Fact Sheet* (Washington, DC, May 25, 2010).

[39] U.S. *Department of Defense, Strategy for Operating in Cyberspace* (Washington, DC, July 2011), 5, 6.

[40] Jim Garamone, "Alexander Details U.S. Cyber Command Gains," September 24, 2010, from American Forces Press Service.

[41] Brigadier General Franz, U.S. Cyber Command/J3, "Cyberspace Operations," lecture, U.S. Army War College, Carlisle Barracks, PA, December 14, 2012, cited with permission of Brigadier General Franz.

[42] Colonel John Surdu, Chief of the Commander's Action Group, U.S. Cyber Command, interview by author, Fort George G. Meade, MD, October 31, 2012. Cheryl Pellerin, "Cybersecurity Involves Federal, Industry Partners, Allies," November 8, 2012, www.defense.gov/news/newsarticle.aspx?id=118479 (accessed December 14, 2012). Tim Maurer, "Is it Legal for the Military to Patrol American Networks?," December 5, 2012.

[43] U.S. Cyber Command, *USCYBERCOM Concept of Operations,* Version 1.0 (October 22, 2011).

[44] General Keith Alexander, Commander, U.S. Cyber Command, "Armed Forces Communications and Electronics Association (AFCEA) TechNet Land Forces Conference/ Cyberspace Operation," August 14, 2012, CSPAN, video file, http://www.c-spanvideo.org/event/206765 (accessed September 2, 2012).

[45] Ibid.

[46] "Cybersecurity Workforce Framework," October 2012, Federal News Radio.

[47] Colonel John Surdu, interview, October 31, 2012.

[48] Lieutenant Colonel Jori Robinson, Commander's Action Group, U.S. Cyber Command, interview by author, Fort George G. Meade, MD, October 31, 2012.

[49] Admiral Gary Roughead, "CNO Guidance for 2010: Executing the Maritime Strategy," (September 2009), 6.

[50] Commander Albert Angel, *Can the Navy's Tenth Fleet Effectively Combat the Cyber Threat?,* Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, March 25, 2010), 13.

[51] VADM Jack Dorsett, Deputy CNO for Information Dominance, quoted in Chief of Naval Personnel Public Affairs, "Information Dominance Corps Warfare Insignia Approved," February 22, 2010, linked from the *United States Fleet Cyber Command/Tenth Fleet Home Page,* http://www.navy.mil/search/display.asp?story_id=51448 (accessed December 4, 2012).

[52] Ibid.

[53] U.S. Fleet Cyber Command, U.S. Tenth Fleet, "Vision," (September 18, 2012), http://www.fcc.navy.mil (accessed September 25, 2012).

[54] U.S. Fleet Cyber Command, U.S. Tenth Fleet, "U.S. Fleet Cyber Command, U.S. Fleet Forces Command Announce Navy Cyber Administrative Realignment," April 18, 2010.

[55] Carlo Munoz, "Navy Restructures Chain of Command for Cyberwarfare Forces," *Defense Daily 250, no 13*, April 19, 2011, http://search.proquest.com/docview/862553592?accountid=4444 (accessed September 12, 2012).

[56] Navy Cyber Forces, "Navy Cyber Forces Mission Statement," www.public.navy.mil/fltfor/cyberfor/pages/mission%20statement.aspx (accessed October 2, 2012).

[57] U.S. Fleet Cyber Command, U.S. Tenth Fleet, "U.S. Fleet Cyber Command Mission," (September 18, 2012), http://www.fcc.navy.mil (accessed September 25, 2012).

[58] Ibid.

[59] Starnes Walker, "U.S. Fleet Cyber Command, U.S. Tenth Fleet," briefing slides to AFCEA, Washington DC, April 2012, http://www.afcea.org/smallbusiness/files/SBPartnershipSymposiumApril2012/2012_AFCEA_CTO_final.pdf (accessed October 20, 2012).

[60] Ibid.

[61] Ibid., U.S. Code, Title 10, Subtitle A, Part 1, Chapter 21, Subchapter II, Section 435.

[62] Starnes Walker, "U.S. Fleet Cyber Command, U.S. Tenth Fleet," April 2012.

[63] Vice Admiral Michael S. Rogers, "Before the Merging Threats and Capabilities of the House Armed Services Committee," *Congressional Record* (July 25, 2012), 4.

[64] Ibid., 5.

[65] Ibid., 5.

[66] U.S. Army, "Army Establishes Army Cyber Command," October 1, 2010, http://www.army.mil/article/46012/army-establishes-army-cyber-command/ (accessed November 18, 2012).

[67] Mr. John M. McHugh, Secretary of the Army and General George W. Casey Jr., United States Army Chief of Staff, *2011 Army Posture Statement* (Washington, DC: The Pentagon, March 2, 2011), https://secureweb2.hqda.pentagon.mil/VDAS_ArmyPostureStatement/2011/index.asp, Army Cyber Command Information Paper.

[68] U.S. Army Cyber Command, "Organization," http://www.arcyber.army.mil/org-arcyber.html (accessed September 25, 2012).

[69] U.S. Army Cyber Command, "ARCYBER Way Ahead," briefing slides, Ft Meade, MD, October 2012.

[70] U.S. Army Cyber Command, "Organization," http://www.arcyber.army.mil/org-arcyber.html (accessed September 25, 2012).

[71] U.S. Army Cyber Command, "1st IO Command," http://www.arcyber.army.mil/org-1stiocmd.html (accessed September 25, 2012).

[72] INSCOM, "Major Subordinate Commands," http://www.inscom.army.mil/MSC/ (accessed September 25, 2012).

[73] Mr. John M. McHugh,*2011 Army Posture Statement*, March 2, 2011).

[74] U.S. Army Cyber Command, "Organization," http://www.arcyber.army.mil/org-arcyber.html (accessed September 25, 2012).

[75] Army Cyber Command/2nd Army AFCEA NOVA IT Day Presentation, "Transforming the Army Enterprise to support the Warfighter," McLean, VA, December 9, 2010, 4.

[76] U.S. Army Cyber Command, *2012 Army Posture Statement Addendum K - Cyberspace: Army Cyber Command and Cyberspace Operations* (Washington, DC: The Pentagon, February 17, 2012).

[77] U.S. Army Cyber Command, “ARCYBER Way Ahead,” briefing slides, Ft Meade, MD, October 2012.

[78] Major General Rhett Hernandez, “Statement of Major General Rhett Hernandez, USA, Incoming Commanding General, U.S. Army Forces Cyber Command Before the House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities, 2nd Session, 111th Congress,” *Congressional Record* (September 23, 2010), 8.

[79] J.R. Wilson, “MARFORCYBER: Marines Fight in a New Domain,” January 5, 2012. www.defensemedianetwork.com/stories/marforcyber-marines-fight-in-a-new-domain/ (accessed December 4, 2012).

[80] Ibid.

[81] Marine Forces Cyber Command, “USMC Cyberspace Update,” AFCEA Quantico-Potomac Chapter, Washington DC (March 31, 2011), 11.

[82] J.R. Wilson, “MARFORCYBER” January 5, 2012.

[83] Ibid.

[84] Amber Corrin, “Cyber Programs at a Glance,” November 17, 2011.

[85] Major General William T. Lord, “USAF Cyberspace Command, To Fly and Fight in Cyberspace,” *Strategic Studies Quarterly* (Fall 2008), 10.

[86] Ibid., 10; Jason Healey, “Claiming the Lost Cyber Heritage,” *Strategic Studies Quarterly* (Fall 2012), 16.

[87] “Cyber Guardian, Collaborating to Advance U.S. Interests in Cyberspace,” *Military Information Technology*, vol 16, issue 10 (November 2012), military-information-www.technology.com/mit-home/…/6138-qaa-gen-alexander.html?tmpl=component&print (accessed December 2, 2012).

[88] Air Force Cyber Command, *Air Force Cyber Command Strategic Vision* (Barksdale AFB, LA: Air Force Cyber Command, February 2008), 14.

[89] “Cyber Guardian, Collaborating to Advance U.S. Interests in Cyberspace,” *Military Information Technology*, vol 16, issue 10 (November 2012), military-information-www.technology.com/mit-home/…/6138-qaa-gen-alexander.html?tmpl=component&print (accessed December 2, 2012).

[90] Ibid.

[91] Mark Cacas, “Stepped Up Cyberthreats Prompt Air Force to Rethink Training, Acquisitions,” November 30, 2012, www.afcea.org/content/?q=node/10392 (accessed December 3, 2012).

[92] “Cyber Guardian, Collaborating to Advance U.S. Interests in Cyberspace,” November 2012.

[93] Secretary of the Air Force Michael Donley and Dr. Mark Maybury, “Air Force Cyber Vision 2025, Assuring the advantage in Air Space and Cyberspace,” *Armed Forces Journal* (October 2012), http://www.armedforcesjournal.com/2012/10/11492950 (accessed October 25, 2012).

[94] Brigadier General Franz, U.S. Cyber Command/J3, “Cyberspace Operations,” lecture, U.S. Army War College, Carlisle Barracks, PA, December 14, 2012, cited with permission of Brigadier General Franz.

[95] Jared Serbu, “Air Force Role Just 1 Piece of DoD’s Cyber Puzzle,” December 3, 2012.

[96] U.S. Joint Chiefs of Staff, Joint Publication 1-02, November 8, 2010, 92.

[97] Jared Serbu, “Air Force Role Just 1 Piece of DoD’s Cyber Puzzle,” December 3, 2012.

[98] U.S. Department of the Air Force, *Implementation of the Secretary of the Air Force Direction to Establish Air Force Cyberspace Command (AFCYBER),”* Program Action Directive 07-08, Change 1 (Washington, DC: U.S. Department of the Air Force, January 24, 2008), 5.